

REMARKS/ARGUMENTS

Claim Amendments

The Applicant has amended claims 1 and 10. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-19 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

Claim Rejections – 35 U.S.C. § 112

Claims 1 and 10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter as the invention. The Applicant has corrected the deficiencies in claims 1 and 10 and the Applicant respectfully submits that claims 1 and 10 are now allowable.

Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1-14 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over WO 02/011467 to Jones et al (hereinafter "Jones") in view of US Patent Publication Number 2003/0051041 to Kalavade et al (hereinafter "Kalavade") and US Patent Number 7,184,764 to Raviv et al (hereinafter "Raviv"). The Applicant respectfully traverses the rejection of these claims. The present invention discloses a Single Sign-On method having distinguishing features which are neither anticipated nor suggested by the cited art.

A typical 'Single Sign-On' (SSO) service (paragraph [0002]) enables users to access different services without the different services explicitly authenticating such users for each particular service. The support of this principle implies in the Internet world that a user provides an identity with a password only once at a given Identity Provider and the resulting authentication is valid for entrance to other services or Service Providers.

As claim 1 of the present invention discloses, when a user attempts to sign on to Service Provider (SP) in a federation of Mobile Network Operators (group of related MNOs), the SP provides a specific URI as a Single Sign-On entry point towards the

federation. The provided SSO point is trusted by the rest of the MNOs in the federation. As the user roams through the federation each Service Provider that receives a sign on request from the user receives a token where the authentication assertion of the user was generated (specific URI). The SP checks that the site is trusted and if so, the user is allowed to log into the SP. In other words, the user can sign on to one of any number of "trusted" sites and any subsequent SP receives notification that the user is authenticated at a trusted site, which is part of the Global Single Sign-On Front End. (para. 79-82) This method comprises the steps of authenticating the user roaming in the visited packet radio network, via a proxy, towards the user's home service network and creating a master session at the user's home service network with Single Sign-On related data.

The Jones reference is cited for disclosing Single Sign-On utilizing a home RADIUS server and broadly interprets Jones configuration as comparable to the G-SSO-FE of the Applicant's present application. "Each wireless access user has a personal computer PC and a UMTS user equipment (UE) 21'and 22' with a directly attached antenna 20 and is connected by typical data connections such as an RS232, USB or Ethernet to the PC." (second paragraph of Detailed Description). However, the user equipment in the Jones reference requires being connected through the Internet by the user's PC to the RADIUS server. The system does not work without this feature. This is not a factor in the Applicant's present invention.

The Kalavade reference is cited for teaching a converged billing/authentication gateway that maintains billing records for a roaming user. Kalavade is also cited for modifying the visited AAA server of Jones to include the capability of binding a user's identifiers with the home AAA server.

Wikipedia discloses that Single Sign-On is a property of access control of multiple, related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. As different applications and resources support different authentication mechanisms, Single Sign-On has to internally translate to and store different credentials compared to what is used for initial authentication.

A Single Sign-On system may be summarized in the following: SSO uses centralized authentication servers that all other applications and systems utilize for authentication purposes, and combines this with techniques to ensure that users do not actively have to enter their credentials more than once.

In a first scenario of SSO, a user is to be authenticated by a first network (or first domain) in order to get free access to a second network (or second domain, or second service) and/or to a third network (or third domain, or third service) and so on. Applying SSO is not a good fit in this situation as there is no requirement to carry out any further authentication of the user after having been authenticated in the first network. SSO in this application provides access to many resources once the user is authenticated, which increases a negative impact in case the credentials are available to other persons and misused. Therefore, Single Sign-On in this instance requires an increased focus on the protection of the user credentials.

In a second scenario; a user has to be authenticated by a first network (or first domain) before accessing a second network (or second domain, or second service) and the user has to be authenticated by the second network before using second network services or before accessing a third network (or third domain, or third service), and so on. In this case there is need for further authentication.

In the first scenario, there is no need for further authentication of the user once the user has been authenticated the first time because the successive entities believe that if the user has gotten this far, the user must be authenticated. Therefore, any cited art whose focus is the use of SSO in the first scenario is not really relevant to the present invention. In this respect, the Jones, Kalavade, and Raviv references all apply in this first scenario where services in different areas from the initial sign-on are accessible after the first authentication and no further authentication is required. The application of SSO as disclosed by the Applicant does not make sense in this scenario.

On the other hand, the Applicant's present invention, applying SSO in the second scenario where authentication of the user is required by each subsequent system, discloses that the original network authenticates the user and the subsequent networks have a mechanism (disclosed above) to verify that the user has been authenticated by

the original network. The present invention addresses scenarios where SSO makes sense and describes a mechanism in terms of a system and a method to allow the user to access the subsequent network (or subsequent service) without requiring a further explicit authentication.

Also, regarding the limitations recited in claim 7; none of the cited references disclose or teach the use of a token received by the user that indicates where the authentication assertion of the user was generated (specific URI). The Examiner did not address this limitation in either the initial Non-Final Office Action or the present Final Office Action. As noted above, the cited references, Jones, Kalavade and Raviv, either individually or in combination do not disclose or teach this limitation,

The Applicant respectfully submits that the cited references do not disclose individually or in combination, the limitations of claims 1 and 10. This being the case, the Applicant respectfully requests the allowance of claims 1 and 10 and since the depending claims contain the same limitations, the Applicant requests the allowance of dependent claims 2-9, 11-14 and 19

Claims 15-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Jones and Kalavade as applied to claims 1-14 above, and further in view of US Patent 6,578,085 to Khalil et al (hereinafter "Khalil"). The Applicant respectfully traverses the rejection of these claims.

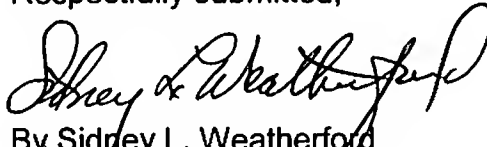
The Khalil reference is cited as disclosing tracking IP addresses assigned by a number of foreign networks and determining visited networks which assigned IP addresses to a user. However, the Applicant respectfully submits that Khalil fails to disclose the missing limitations, as described above that are lacking in the cited references Jones and Kalavade. Without the described limitations, the combination of Jones, Kalavade and Khalil fail to disclose or teach, individually or in combination, the limitations of claim 10 and thus claims 15-18.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



By Sidney L. Weatherford
Registration No. 45,602

Date:

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-8656
sidney.weatherford@ericsson.com